VZCZCXRO4658
PP RUEHBI RUEHCI
DE RUEHNE #1670/01 0691043
ZNR UUUUU ZZH
P 101043Z MAR 06
FM AMEMBASSY NEW DELHI
TO RUEHC/SECSTATE WASHDC PRIORITY 1102
INFO RUEHCI/AMCONSUL CALCUTTA 2290
RUEHCG/AMCONSUL CHENNAI 2136
RUEHBI/AMCONSUL MUMBAI 1366
RUEAWJA/DEPT OF JUSTICE WASHDC
RHEHNSC/NSC WASHDC
RUEIDN/DNI WASHINGTON DC
RHHMUNA/CDR USPACOM HONOLULU HI
RHHJJPI/PACOM IDHS HONOLULU HI
RHMFISS/HQ USSOCOM MACDILL AFB FL
RHMFISS/HQ USCENTCOM MACDILL AFB FL
RUEKJCS/SECDEF WASHDC
RUEKJCS/JOINT STAFF WASHDC

UNCLAS SECTION 01 OF 02 NEW DELHI 001670

SIPDIS

SIPDIS

STATE PM FOR MMARKOFF AND ERUSSELL

E.O. 12958: N/A
TAGS: PREL PGOV KCIP TINT PINR IN
SUBJECT: A REVISIT TO INDIA'S CYBERSECURITY "CERT-IN" FACILITY

REF: 04 NEW DELHI 6953

¶1. Poloff on February 16 briefly revisited India's Computer Emergency Response Team (CERT-In) facility (Reftel) and made the following observations:

Security

¶2. Nearly all interior doorways were secured with an infra-red badge reader, including every door that led to a room housing computer equipment. All observed CERT-In employees wore (visibly) either green or yellow badges; Poloff did not ask about the distinction between the two kinds of badge.

¶3. Access to the Network Operations Center and the Server Room nested inside it were both controlled by two-factor security, a badge-reader and biometric thumbprint scanner. The Server Room contains at least 10 IBM and 6 Sun servers, labeled either "Web," "Firewall," "Anti-Virus" or "Proxy."

¶4. Each hallway Poloff walked down, and nearly every intersection of hallways, was monitored by a ceiling-mounted closed-circuit camera. One video monitor station was inside a glass-enclosed security room; the monitor was fed by 16-20 cameras, some of which were located outside, according to the images displayed on the monitor.

¶5. CERT-In did not secure its front door during business hours. Poloff was left unattended in the reception area for 5-10 minutes after arrival. All doors stemming from the hallway past the reception area required badge access.

¶6. CERT-In has an X-ray machine in the reception area, but it was unattended and not used during the visit.

Personnel and Bio-Data

¶7. CERT-In has (since at least October 2005) a new director -- Dr. Gulshan Rai -- but many of the same employees, including Operations Manager Anil Sagar (Reftel), remain. Dr. Rai has since the late 1990s written several papers on cybersecurity, including on cryptography and integrating IT with standard educational curricula. He is a member of the Ministry of Communications and Information Technology/Department of Information Technology (DIT) Inter-Ministerial Working Group on Cybersecurity Education and Awareness.

¶8. Dr. Rai also serves as Executive Director for ERNET, an autonomous society within the DIT; in this capacity he reports directly to the seniormost civil servant in the DIT, the Secretary. ERNET's mandate includes integrating IT into school curricula. It also possesses India's largest land- and satellite-based IT network linking educational and research institutions. ERNET was inaugurated in 1986 in the GOI's Department of Electronics as a GOI-UNDP joint venture.

Operations

¶9. Sagar told Poloff that CERT-In runs 1-2 day training courses on specific functions, such as preventing phishing attacks, approximately once per month.

¶10. Sagar also claimed www.cert-in.org.in has approximately six million Indian users.

¶11. Fourteen people were at work on workstations in the Network Operations Center. Six additional workstations were unused.

CERT-In Powers and Functions

¶12. Rai told Poloff that the IT Act (2000) gives CERT-In the

NEW DELHI 00001670 002 OF 002

authority to force an ISP to block Indian web sites that violate Indian law, including for hosting pornography. If the offending web site is in another country, CERT-In is authorized to request that the hosting country investigate the matter.

Follow-Up

¶13. Poloff plans one more visit to CERT-In in the next few months, and will gladly take questions or look out for specific observables. Poloff's classified e-mail address is madnickhj@state.sgov.gov.

¶14. Visit New Delhi's Classified Website:
(http://www.state.sgov.gov/p/sa/newdelhi/)
BLAKE